2000

PREPARED BY THE STAFF OF:
ASSEMBLY COMMITTEE ON
INFORMATION TECHNOLOGY

HONORABLE
JOHN DUTRA, CHAIR

The Year 2000 Problem: Local Government and Critical Infrastructure Preparedness

Prepared by
The California State Assembly
Committee on Information Technology

The Honorable John A. Dutra,
Chair

July 28, 1999
State Capitol, Sacramento, CA

Table of Contents

Executive Summary

Local governments and critical infrastructure providers are, on the whole, well down the road to successful management and containment of the Year 2000 Problem.

The Year 2000 Problem is manageable, as long as the seriousness, urgency, commitment and due diligence that it commands are recognized. The host of issues to be addressed in response to potential Year 2000 Problem, or "Y2K", failures can be so overwhelming as to render the very thought of successful Y2K management an exercise in futility. Fortunately, given the responses and testimony provided to the Committee in hearings conducted across the state there is room for more than guarded optimism.

Cities, counties, utilities, public safety agencies, and other transportation infrastructure providers are taking the Year 2000 Problem very seriously and developing aggressive remediation and continuity planning programs. Many entities are on-track with their preparedness programs; internal remediation, testing, and systems replacement is well underway statewide. Without exception, all entities before the Committee have adopted either a working continuity plan or a timeline for the implementation of one. The coordination of efforts between geographically and politically overlapping or contiguous entities, vendors, utilities, and data exchange partners, most notably the state of California itself, varies greatly from one to another. Virtually every group has created a public outreach and awareness program, however, the breadth and scope of these programs are, to date, seriously inadequate.

Cities and counties have devoted an amazing amount of money and time to making sure that their programs are not only complete but adequately comprehensive. For example, the County of Los Angeles has budgeted over $155 million on their remediation program alone. At the other end of the spectrum, the small City of Anderson had to borrow $50,000 to cover the costs of implementing its program. In light of the serious financial difficulties that local governments grapple with on a regular basis, these funding commitments represent the priority that local governments of all sizes have placed on the successful implementation of their Y2K plans.

In the development phase of the continuity planning process, many local governments are following the lead of established, successful preparedness programs from around the country. Local governments like the City of Lubbock, Texas and Montgomery County, Maryland have been profiled in the national press as model Y2K planning communities and have led the way in table top drills and coordinated business continuity planning. Both were also present at the state Department of Information Technology and Office of Emergency Services Business Continuity Planning Conference held in Sacramento earlier this year. The Conference was attended by over 1000 state and local officials and was

cited as an essential component of the planning process by many who testified before the Committee.

It is reassuring that public safety agencies, without exception, have extreme confidence in their ability to respond to any potential problems linked to Y2K and in the strength of their business continuity plans. To their credit, law enforcement and fire officials have learned lessons from the major calamities and events that have been endemic to life in California since its founding 150 years ago. The State of California and local governments have also created and successfully implemented mutual aid agreements in order to speed response to major events. These mutual aid regions have provided a perfect backdrop for successful joint contingency planning and multi-agency table top drills to occur as a matter of course.

The state's transportation authorities and airports have been involved in various planning efforts for Y2K with federal officials and local government and planning agencies in primary service areas, even if those organizations are not represented on the authority's board. Airports have been a source of concern in the popular press and among many local officials, and the pressure put on airport administrators to become Y2K compliant as soon as possible has resulted in aggressive testing for embedded systems failures. Transit agencies, once their buses and trains are certified compliant by vendors, have business continuity planning as their number one priority in order to maintain a constant level of service to the public.

At the direction of the Public Utilities Commission, utilities have a standard timeline for completion of their remediation activities and the development of a comprehensive continuity plan. Under the leadership of the North American Electric Reliability Council (NERC), one critical industry-wide table top drill was run successfully on April 9th and an industry-wide test is planned for September 9th. The good news that is echoed by every company that provides these critical services to the public is that there will not be severe blackouts, phone outages, or water disruptions. However, on a case-by-case basis each utility and every utility company still has specific Y2K issues outstanding, some significant enough to have major employers and manufacturers worried about their ability to conduct business come Monday, January 3, 2000. Most notably, the industry as a whole has a tremendous amount of work to do in the arena of public outreach and awareness regarding their overall level of preparedness for the Year 2000.

The Committee has been concerned with the efforts that local governments have taken to coordinate activities with overlapping and contiguous agencies, vendors, and their critical infrastructure partners. There are many different aspects to the coordination equation; these include end-to-end testing and systems compliance issues, business continuity planning, emergency response equations, vendor certification, and the like.

The state Department of Information Technology (DOIT) has taken lead in coordinating comprehensive end-to-end systems testing. The Department has developed a multi-pronged, coordinated approach to end-to-end systems testing and remediation. Potentially, each interface between the state and a local government could raise

additional resource and preparedness questions, if not properly addressed, threatening the success of the preparedness program.

Within each local government or critical infrastructure entity a determination needs to be made regarding the level to which integrated systems testing is necessary, the degree to which the organization relies on others for services critical to business continuity, and how they can be of assistance to or be assisted by neighbors, entities with common constituencies, or vendors. It became apparent that while business continuity plans have been and will continue to be developed, these crucial determinations have not been included in those planning processes as a matter of course.

Most cities and counties have either formed working groups or have been meeting on a semi-regular basis, but that does not mean that there have been detailed discussions regarding data exchange issues, business continuity planning, determinations regarding the impacts that may occur on shared resources or service providers, or public awareness issues. Positive movement, again, has been made by public safety agencies who have worked within a mutual aid context for some time giving them an incentive to make their business continuity plans coordinated from the start.

Risk assessments regarding the likelihood of a major utility breakdown or a failure to provide power, telecommunications, or water on a limited basis are a critical part of every business continuity planning process. The utility companies have begun to factor these potential scenarios into their business continuity plans as they themselves are major customers of other utility companies. Positive steps taken by the California Legislature and by the White House and Congress have helped give utilities the protections that they needed to develop comprehensive preparedness and business continuity plans.

Vendor relationships and systems certifications are critical to the development of a successful remediation program, especially for those providers of critical infrastructure. Vendor certifications are crucial to transportation authorities whose preparedness questions and lingering doubts stem from the potential for embedded systems failures.

Many small local governments do not have in-house programmers and end up completely dependent on vendors for their Year 2000 Problem remediation and testing. The lack of in-house programmers also has rendered small governments likely targets of frivolous litigation. To that end, testimony provided by the Association of Bay Area Governments (ABAG) called for limited liability relief for these entities. Presumably, even though they don't have the same level of control over automation projects that some larger entities will have, smaller governments may be held just as liable, if a vendor fails to remediate a critical system.

Between the technical aspects of identifying data exchange partners and conducting thorough end-to-end testing for automated systems and their accompanying business continuity plans, increased coordination will need to occur sooner than later. There also remains the amazingly delicate task of developing coordinated public awareness messages and communications campaigns across the state.

Generally, every city and county that has the budget to do so has created a Year 2000 brochure for general distribution to the public. Utilities have been dropping inserts in billing statements. The American Red Cross has developed a readiness guide intended to help people become better prepared specifically for Y2K. Police and Sheriff's departments have developed materials to keep citizens aware of potential scams and the dangers associated with risky preparedness practices. The Air Transport Association is developing a media response to unreasonable claims that planes will fall out of the sky. In addition, the state, the federal government, the U.S. Chamber and several other industry groups are also beginning their own public awareness campaigns regarding the real issues and risks posed by the Year 2000 Problem. And, of course, everyone who's anyone has a Y2K homepage.

While the messages of preparedness and confidence generally expressed in these brochures and materials are accurate and well thought out, the abundance of different messages circulating throughout the state are astounding. There is a strong likelihood that our public safety officials are telling individuals one thing, while a county office of emergency services advises against it, but for reasons which contradict those in a utility billing insert, which was written to address concerns raised by the previous evening's eleven o'clock news.

Ironically, despite all of these varied public awareness campaigns that are already in place, there is an overwhelming need for more public awareness of Y2K and the potential issues that accompany it. In fact, most entities need to create more aggressive outreach programs to the media and the public, devote more time and energy towards developing a consistent message with other entities that provide services to the same population. Governor Davis's Year 2000 Executive Order, D-3-99, establishes a Year 2000 Communications and Outreach Task Force with the charge of working with DOIT, local governments, and private industry to coordinate themes and messages for Y2K awareness.

In sum, local governments and critical infrastructure are taking the Year 2000 Problem with an appropriate level of seriousness and urgency. The methodology of the private sector and large government agencies has been adopted by entities across the state, large and small. The good news is that there is still time to address outstanding issues that have been raised within the process of remediating existing problems. The bad news is that there are no deadline extensions for those who fail to recognize that outstanding issues do indeed exist.

Preparedness Report Card

Based on testimony and materials provided at public hearings at seven locations across the state, the Committee has assigned the following "grades" to the current level of preparedness of cities, counties, utilities, public safety agencies, and transportation infrastructure:

	Overall Preparedness	**Progress Within Organization**	**Coordination with Other Entities**	**Business Continuity Planning**	**Public Awareness Efforts**
Cities	***B+***	A	B-	A-	B+
Counties	***B***	A-	C+	B+	B
Public Safety Agencies	***A***	A	A	A	B
Transportation	***C+***	C+	C+	B	C
Utilities	***B***	A-	B-	A-	C

I. City Preparedness

"We are confident that our mission critical systems will be supporting public safety, finance and other operations in the year 2000. Further, we don't anticipate any major problems in the key utility areas such as power, water or communications. Essentially, what is vital, and what our biggest concern is, when it comes to the year 2000 is that our message [of preparedness] does not get distorted."

Kevin Corcoran, City of Los Angeles

California's cities are implementing comprehensive Year 2000 Problem programs. Many have completed, or very nearly completed, their internal systems remediation and identified the risks of failure for Y2K impacted resources. Most are in the midst of, or have recently finished, testing their proprietary systems and putting them back into production. Business continuity plans are being developed to protect against a disruption in services to the public should failures occur.

Cities' inventorying processes are similar to those at most large corporations, as there is a wide variety of resources that could potentially be impacted by Y2K. For the most part, comprehensive systems inventories survey the following: large automation systems, server hardware, operating systems, application software, PC hardware, PC operating systems, embedded systems and chips, communication systems, and, when services are procured directly from vendors, vendor compliance.

All Y2K programs must begin with a comprehensive inventorying process, followed with a prioritization of those impacted systems, and then the subsequent remediation and testing of those systems in the order of priority.

For cities with complex automated systems, or simply large populations, the baseline for completion of each step from inventorying to putting programs back into production can only be expressed in years from the time of implementation. For instance:

> "The City of San Diego started [on its Y2K program] in 1996, with a complete inventory of all of our major enterprise software systems, critical applications on the computer. Late in that year a project team was organized at the San Diego Data Processing Corporation, and in early 1997, additional consulting help was acquired from the outside. All of our mainframe applications, our major, most critical business applications have been finished and tested, and put back into production in the last two months."

For larger cities, the results of these inventories produced mind-boggling administrative tasks. For smaller cities these inventories produced a subsequent list of projects that they had no realistic way of administering themselves. Because their software was most likely purchased "off the shelf" to begin with, many smaller cities must rely on vendors to provide the required remediation.

In determining how to address the results of inventories, cities needed to evaluate and prioritize all resources which were identified as impacted by Y2K and identify the resources that would be used to mitigate those impacts. Specific to the City of Fresno:

> "When we did the analysis of our 196 non-compliant issues we found that it was going to take about 65,000 hours to fix or repair them, but as you know you can't just fix things -- when you come to them you're going to find things you have to improve. These enhancements were going to take another 25,000 hours. That doesn't include the embedded chips and the pumps in elevators and things that we have to look at and find. It doesn't include things out of our control, and other interface issues which we were concerned about."

Those cities, like San Diego, which chose to primarily remediate their existing systems have relied on additional, outside consultants to assist with their Year 2000 testing and remediation. The City of Sacramento became very dependent on working with their vendors to alleviate potential embedded chip failures – in fact, the City was working exclusively through vendors to complete their inventory and remediation processes.

Most City Councils and Mayors have taken the responsible position of "owning" the problem directly, meaning that they have appointed one official to handle Year 2000 Problem issues who reports directly to the Council or the Mayor. For smaller cities, this usually means that the City Manager is also the Year 2000 Project Manager. For larger cities, this can mean either the city CIO or another individual is given the responsibility of operating a Y2K project office.

The fact that Y2K issues are given a high priority within cities' governing bodies is reflected in the support for remediation and continuity planning in city budgets. Accordingly, the estimated spending levels for several cities on Year 2000 Problem compliance and planning operations reflects its priority status. (See Appendix H)

These budgeted amounts do not necessarily reflect total spending on Y2K by these cities, as determining the true costs of Y2K is next to impossible. Many entities use Y2K as an impending event to replace existing systems, making much needed upgrades a matter of necessity. For example, the City of Fresno, taking the replacement philosophy to its logical extreme: replaced just about every system in its inventory that had compliance issues and made the required related upgrades in Year 2000 compliant systems as well. The result was an additional investment of somewhere between six and ten million dollars.

For those municipalities which do not have the luxury of finding several additional million dollars in their budget, Y2K project funds were created by diversions from other

projects or reserve funds. In one instance, the City of Anderson (population ~9,000), located in Shasta County, had to borrow $50,000 to cover Year 2000 preparedness costs after $70,000 had been taken from the city's limited reserve. For small cities like these, Year 2000 financial burdens have compounded existing dilemmas that have plagued local governments since the passage of Proposition 13.

The level of systems integration that cities have with external agencies, utilities, and vendors varies greatly across the state. For those cities with municipal utilities, those specific city departments have a high level of systems integration (see section V). Many cities have extensive contracting agreements with county law enforcement agencies or special districts for service. Every city has a number of vendors on which it relies for basic provisions of goods and services, yet the degree to which these contracts factor into their remediation plans vary just as widely as the existence of the contracts.

Unlike the disparate levels of integration and coordination that needs to occur on the integrated systems and remediation level for cities, the coordination that is crucial to successful business continuity planning does not vary across the state. Every city is a member of a political and physical geography of multiple political jurisdictions, multiple utility service areas, and regional mutual aid. While many of these city issues revolve around public safety (see section III), there is an essential planning element at the city level that is defined by their existing relationships with other cities, the county, utilities, local law enforcement contracts, and vendor contracts.

This required level of coordination should not surprise anyone, much less those involved in any type of emergency planning or public safety administration. For high level coordination to occur, cities themselves need to have reached a point where they can readily identify resources potentially impacted by Y2K failures. The easy way to determine which of these resources would also be potentially crucial for reacting within a coordinated context is to consult the completed business continuity plan.

Many continuity plans are adaptations of existing contingency and disaster plans that would have been in use in the case of a non-Y2K related problem. Modifying existing plans to fit the profile that has been developed through the inventory process is only half of the battle, however. Year 2000-specific continuity plans need to account for Year 2000-specific issues; in other words, if a system is not compliant it is not going to come back on-line when the power gets restored like it would in a severe winter storm. Cities may also find that they have need to broaden the universe of contingencies that they are developing plans for. The City of Fremont found this to be the case when officials there decided that they would include a nuclear reactor leak at Lawrence Livermore labs in their regimen of potential Year 2000 related events to be prepared for.

The City of Tracy was not unique in its approach to developing contingency plans that rely exclusively on internal agencies rather than on mutual aid partners. The feeling prompting this approach that they need to be able to stand on their own and not expect external agencies or the state to help them out because external agencies will have their own worries.

Regardless, cities in the state are still members of regional planning agencies and mutual aid regions. Many of these groups have set up initial "table top" drills where they can run through their respective continuity plans in parallel. These often include local law enforcement, local hospitals, utilities, and a number of local governments. Earlier this year the City of Los Angeles held a citywide contingency planning exercise that not only included representatives from these groups but also the grocery, personal banking and finance industries, transportation providers and members of the media.

These regional planning and mutual aid groups are also spearheading several coordinated outreach campaigns that are underway across the state. The City of Oakland, for example, is developing a model for community and neighborhood groups throughout the Bay Area to promote disaster preparedness and personal safety in case of a disaster in general.

Public awareness programs have been implemented by almost every city which testified before the committee. However, these programs, should they fail to be transformed into effective awareness campaigns, may ultimately do little to make the public truly aware of the state of our Y2K preparedness.

While the most popular way to disseminate information to the public is through brochures and posting information on the city's homepage, local cable programs, town hall meetings, and preparedness fairs are being held throughout the state. Brochures are generally kept in public buildings, such as the library and city hall, or passed out at schools and special events. Multiple brochures are being made available on specific Y2K issues (preparedness at home, small business assistance) and in a variety of languages.

Local officials in cities with the adequate level of resources have been able to initiate outreach programs to explain how the city is preparing for Y2K directly to citizens groups, chambers of commerce, and religious groups. In those communities where City Council proceedings are broadcast over local cable access channels, citizens have had the opportunity to see city-specific Y2K discussions.

The City of Lodi has held monthly Y2K forums with the public where panels of speakers from various private and public sector entities discuss their remediation status and preparedness issues. Speakers have included representatives from banks, hospitals, fire departments, utilities, water services, grocery stores, electric services, the American Red Cross, and more.

The City of Santa Monica has developed a unique approach to creating public awareness by taking an aggressive approach to getting into the schools and providing factual information to children. By employing a "be prepared, don't be scared" concept, children will have an understanding about the New Year that balances the rumors, exaggeration, and reports in the media. Children will then also have the opportunity to take home materials from school regarding the preparedness of the community for Y2K.

II. County Preparedness

"We expected the worst, and we were gratified that the problems and concerns that we did unearth were ultimately very manageable."

Bob Geise, Orange County Grand Jury

"One of the challenges that we have found in our overlaps between the state and local governments has been addressing the interfaces between the counties and the state, and vice-versa."

Elias Cortez, Chief Information Officer of California

Like cities, California's counties are implementing comprehensive Year 2000 Problem programs. Many have completed, or very nearly completed, their internal systems remediation and identified the risks of failure for Y2K impacted resources. Most are in the midst of, or have recently finished, testing their proprietary systems and putting them back into production. Business continuity plans are being developed to protect against a disruption in services to the public should failures occur.

Again, like cities, counties' inventorying process is similar to those at most large corporations as there is a wide variety of resources that could potentially be impacted by Y2K. For the most part, comprehensive systems inventories survey large automation systems, server hardware, operating systems, application software, PC hardware, PC operating systems, embedded systems and chips, communication systems, and when services are procured directly from vendors, vendor compliance.

However, unlike cities, counties provide a larger array of services on a greater scale. Counties are the primary administrators of state social policy and in that capacity have a large number of interfaces with the state departments. Immediately, the coordination of integrated systems testing becomes an issue for both the state and counties to truly declare themselves Year 2000 ready. The termination of the Statewide Automated Child Support System last year illustrates the issues distinctly; the state and counties must coordinate their automation activities or social policies fail.

Large counties in California provide more social services than many states and thus have the potential Y2K issues that come with the automated systems to make these "county-states" operate like one as well.

The County of Los Angeles alone maintains 98,000 computer programs, approximately 34,000 of which were identified as impacted by Y2K and needing remediation. The County runs the second largest hospital system in the country, and therefore has over 35,000 pieces of medical equipment with embedded systems issues. With over 2700 owned and leased facilities and 35,000 personal computers, the County's $155 million budget for Year 2000 Problem remediation no longer seems quite so large.

The complexity of many large counties' Year 2000 program has prompted Boards of Supervisors to place their CAO or CIO in charge of their program. Large counties that provided testimony to the committee were less confident when it came to the issues of coordination and communication than cities but ahead of the game when it came to the remediation of their proprietary systems. As testament to the complexity of the issues surrounding counties' Year 2000 programs several county grand juries, including Orange and Ventura, have taken to self-auditing their own progress.

Upon the completion of basic inventory, critical systems were prioritized to determine the manner in which the remediation process would go forward. From mainframes to personal computers and embedded chips, those that were impacted by Y2K would need to be replaced or made compliant as soon as possible. Most counties have included systems replacement as part of their remediation, when it was technically feasible and economically appropriate.

Y2K issues are given very high priority among all counties, large and small. Boards have supported substantial budgets for remediation and continuity planning. Estimated spending levels for several counties on Year 2000 Problem compliance and planning operations reflects its priority status (see Appendix H).

Counties are actively and aggressively addressing Y2K systems remediation on all proprietary systems. Most are clearly through the bulk of their testing phases and are putting systems back into production, with some exceptions. The programs seem to be in a position where they should be scheduling advanced end-to-end testing with the state in order to become fully compliant for all of those systems that are otherwise complete.

The level of systems integration that large counties are expected to develop with external agencies, utilities, and vendors is greater than that expected to be developed by cities. This should not be a surprise to anyone. Not only do counties have a tremendous amount of external interfaces and data exchange issues, and encompass a broader scope of activities from law enforcement to health care to welfare to emergency services, but they also encompass more geographic and political space.

The complexity of interfaces for smaller counties is not nearly so daunting for several reasons. One, for the really small counties the state often assumes responsibility for programs itself, creating an unusual circumstance of agency to agency interaction on behalf of the county. Two, the large automated systems with million-member databases are generaly non-proprietary to smaller counties. Three, the program environment is

almost always more manageable in terms of developing a reasonable work around for business continuity planning.

Not only is coordination crucial for integrated systems and remediation success, but additional coordination is crucial to successful business continuity planning as well. While public safety coordination is essential (see section III), because the county provides basic services to the community the participation of counties in the planning process is a key to successful implementation of any emergency plan. This required level of coordination should be expected of those involved in any type of emergency planning or public safety administration. Counties for the most part have reached a level where they can readily identify resources potentially impacted by Y2K failures.

Fortunately, large counties and smaller county consortia are already required to participate and administer the state's standardized emergency management system (SEMS). The current emergency management planning processes mandated through SEMS ties in continuity planning and emergency services to develop a coordinated response plan. Agencies work cooperatively to secure communications, fueling, and facilities plans for emergency services, urgent medical care and emergency medical transport, hazardous materials, and basic law enforcement. (See section III).

Counties are modifying existing plans to match the priorities and needs identified through the remediation and testing processes. Aside from law enforcement, the basic services that need to be accounted for in county business continuity plans are emergency services, child protection, adult protection, health care, and emergency food, shelter and water.

The response rates to counties' inquiries of their vendors and suppliers regarding compliance levels have, curiously, varied greatly across the state. While Orange County has received an amazing 100% rate of response to their inquiries, Kern County reported a 40% response rate, and Santa Clara and Alameda Counties were reporting 35% response rates. Orange County aside, the majority of the counties have sent additional letters out or followed up with phone calls to check the status of Y2K certifications as soon as possible.

As with cities, public awareness programs have been implemented by almost every county which testified before the committee. More County Boards of Supervisors have their proceedings broadcast over local cable access channels than city councils; inevitably, citizens who are interested have had the opportunity to see Y2K issues specific to their county brought up in the Board chambers. Like most other local governments and businesses, counties have also created websites, brochures, bill inserts, public meetings, and television and radio spots.

Communications within counties, with contiguous counties, or with others in shared service regions, are crucial to developing comprehensive business continuity plans and consistent messages to the public. Counties have developed several different methods for improving inter-entity communications. In this regard, several counties have convened conferences where all of the cities and county departments could discuss Y2K specific

issues together, including the preparedness of shared resources and the status of critical infrastructure providers, other than themselves.

Counties, however, should pay attention not to confuse the public by publishing that they are “98% complete,” when complete only means that they are finished with internal remediation and testing. These systems are not completed if they cannot be described as Year 2000 compliant. The interfaces that counties and the state maintain need to be addressed through end-to-end testing that has not yet occurred, consequently, these applications cannot responsibly be deemed completed until the proper testing has occurred. As an example, the Orange County Municipal Courts System, which has several DMV interfaces, may be fully Y2K tested and put back into production from the County's proprietary side, but until the interface to the DMV is tested as well it is not a “complete” project.

The Department of Information Technology (DOIT) has created a registry of interfaces by state department, and the registry identifies the number of interfaces that each department has with specific counties (see Appendix J). These interfaces with the state have not been addressed through end-to-end testing for any county as of yet. Discounting for the lack of such testing, many counties have a lower percentage of Y2K “completed” systems than that reported to the Committee. However, the good news is that the great majority of the most rigorous and time consuming testing and remediation has indeed been completed. Furthermore, the counties that testified before the committee were committed to working in partnership with DOIT to completely address all outstanding external interface issues as soon as possible.

III. Public Safety Preparedness

"We look at Y2K as just another event that you have to plan and train for."
Kenneth Henius, Alameda County Fire Department

As Californians, we have lived through all types of emergencies including earthquakes, fires, floods, vicious winter storms, perennial droughts, and our share of civil unrest. Saddled with the task of protecting over 30 million citizens everyday, our public safety agencies and officers are well prepared to create comprehensive business continuity and pubic awareness plans. Public safety agencies depend on each other for assistance in times of need whether that be as security for a Super Bowl or as a member of a California National Guard contingent.

Testimony before the Committee was consistent across the state that, in terms of business continuity planning and joint contingency planning, Y2K is really an extension of existing emergency preparedness for local governments.

Public safety officials are modifying their existing contingency plans for the Year 2000 and further refining these contingency plans as the end of the year approaches. The emergency service personnel are primarily working within their respective city or county law enforcement or OES missions in addition to their response to mutual aid region requests for joint planning exercises.

So that their mutual aid partners are ready for anything and everything, for example, the County of San Bernardino has developed a generic contingency plan for Y2K and distributed it throughout the county. The generic plan can then be quickly customized and adopted by other entities as their own. This type of innovative approach not only allows multiple jurisdictions to efficiently take advantage of another's expertise, but adds value to the joint contingency planning process. In this instance, San Bernadino County, by limiting the potential that it will be called upon to provide mutual aid, has created a circumstance where they may be able to better focus on potential issues at home.

Regional Y2K exercises and scenarios are going to be used to test existing contingency plans as well as specialized training and instructions given to personnel. In the Bay Area, Alameda, Contra Costa, San Francisco, San Mateo and Santa Clara Counties are all planning to complete tabletop drills this summer and early fall. Police and sheriff's representatives expressed a high level of confidence in individual county by county business continuity plans in light of the high level of coordination implemented by law enforcement when addressing everything from civil unrest in the 1960s, to major power outages, the Oakland hills fires, and the Loma Prieta earthquake.

In Los Angeles County cities work in conjunction with one another and County officials within a unique set of mutual aid Areas. Administered by a coordinator from a City within the Area, each coordinator is responsible for interacting with his or her colleagues in contiguous cities and the county in the emergency planning process. For Y2K, Area coordinators, in addition to their normal planning duties, have begun to set up regional business continuity plans and basic exercises to validate their planning methodologies. For instance, when Area "A", coordinated by the City of Santa Monica, conducted a tabletop exercise earlier this year, participants included: cities in Area "A", County officials, Southern California Edison, Metropolitan Water District, American Red Cross, Salvation Army, UCLA Medical Center, Santa Monica Malibu School District, and volunteer groups including ham radio operators and the Santa Monica City Air Corps.

There are also two unique planning considerations in San Diego that have been taken into consideration when contemplating their continuity planning and public safety preparedness: one, the large concentration of military personnel and facilities; and two, the proximity of the Mexican border. The Miramar and Camp Pendleton operations officers are directly involved in joint planning activities underway in San Diego County. In addition, the City of San Diego is required through mutual aid agreements to provide critical services and resources like fire protection to naval facilities within the city limits. Likewise, Tijuana's Office of Civil Defense has been cooperating with the San Diego County Disaster Preparedness Office, and has toured the County's emergency operations center and been given copies of the county's strategic business continuity plan. Moreover, the Tijuana and San Diego city managers have a public planning and coordination committee with which law enforcement regularly discusses a number of operational issues surrounding Y2K. However, while there is cross-border coordination of planning there are few services in the law enforcement arena that San Diego area officials can provide to Tijuana in the event of a real emergency.

Within the public safety agencies themselves, comprehensive remediation work has been underway for some time. County Sheriffs and city police departments have completed inventories for most of their major systems and identified the areas that are in need of remediation. Based on testimony provided to the Committee, public safety agencies have either resolved or are planning to resolve the vast number of Y2K related issues involving critical emergency preparedness facilities, systems, and services within the next several months.

Of some alarm to the public has been the fact that two of the critical resources impacted by Y2K, almost universally, include the 911 switchboard and individual departments' computer automated dispatch systems (CADS).

The remediation of local 911 switchboards is dependent upon the success of telecommunications companies to address and resolve their internal Y2K issues. While 911 systems will, by all accounts, be Year 2000 compliant statewide. Local emergency managers have lost communication with the 911 system during power outages in the past, thus, it is an operational contingency for which they are prepared and have dealt with

before. In addition, some jurisdictions, such as the City of Eureka, are developing cellular-based alternatives to regular phone service for 911 calls, thus increasing operability in the field for officers at the switchboard and decreasing the risk that a power failure will deliver a fatal blow to the 911 system.

Computer automated dispatch systems come in many shapes and sizes, the good majority of which, it turns out, are not Y2K compliant. These dispatch systems either need to be replaced or public safety agencies need to create very high level, comprehensive business continuity plans. Police and sheriff's departments have very efficient continuity plans in place for potential CADS failures at present because an inability to dispatch officers would represent a total breakdown in the ability of our public safety agencies' ability to function. Most often, the manual work around for a CADS failure is working with dispatch cards, a process that is still in use in many smaller law enforcement agencies.

Not surprisingly, the remaining area of heightened concern within the public safety community is the embedded chip problem. There is concern that some of their emergency apparatus may experience an embedded systems failure when responding to an emergency – a fear that many individuals have in the field regardless of the Y2K problem. EMS and fire officials have specific issues surrounding such crucial public safety devices as cardiac defibrillators. During several inventorying processes it was found that many defibrillators, probably one of the most crucial components of any large, advanced life support system, are not Y2K compliant.

Departments are looking at internal business continuity plans as well as community wide planning. They will operate on a log system, paper, and pen and pencil instead of technology if necessary even if, in the case of a CADS failure, that means writing all calls on a card. Additional technical staff will be in attendance all night, in order to deal with any emergencies that may arise from a systems failure. Many public safety agencies are staffing up an emergency operations center, or EOC, as well as alternative command centers, should a problem arise.

There will also be plenty of non-technical staff on duty New Year's Eve, 1999. Most public safety agencies have canceled all vacations for personnel between mid-December to mid-January to not only anticipate potential Year 2000 related events but to respond to what will be an overwhelming demand for additional crowd control. Los Angeles County alone is planning to have more than 9 separate venues with 100,000 plus celebrants.

In addition, there is always the possibility that special circumstances associated with large parties, such as these, may contribute to an accident that could be falsely attributed to Y2K. Should an overzealous party-attendee get into an accident with an innocent power pole, the first, but incorrect, inclination when the power goes out would be to blame the outage on a Y2K failure.

Other potential problems may be associated with Y2K despite the fact that they are essentially public safety problems. For example, individuals going out and buying a

generator and then connecting it straight to the house's wiring could cause electrical fires when the energy company restores power to your home. Individuals may decide to stockpile gasoline in their garage – which could not only pose a serious health risk but also cause explosions if placed too near the water heater.

Along with these unintended consequences of preparedness come those unscrupulous individuals who would use the Year 2000 Problem as a clever device to part the unsuspecting with portions of their life savings. With a large senior citizen population, a major focus of the El Cajon Police Department has been to advise the community how to be on the look out for potential fraud associated with Y2K preparedness, but still be adequately prepared. They have invited speakers to their community meetings and taught members how to properly prepare for any emergency, not just Y2K, and how to identify con artists and scams. The public has received brochures and resource numbers they can call upon with questions and concerns that they may face with Y2K.

The best way to avert power outages caused by errant drivers being blamed on Y2K, houses burning down, gasoline exploding, and widespread fraud is through an effective and coordinated public awareness campaign by public safety agencies. In fact, local government Public Information Officers will most likely not be able to handle all of the inquiries that may arise on January 1st unless there is a comprehensive public information process in place.

One critical aspect of a successful public awareness campaign is the extent to which community groups become involved in the training and education process. Many public safety agencies have been convening public meetings for people to get involved in the community and learn how to be ready for anything. Aggressive community outreach programs by the Oakland Fire Department, in particular, have been adopted by neighboring cities and were helpful in the planning processes undertaken by Alameda County.

Community outreach in several communities means inviting the public to volunteer and participate in tabletop exercises, in order to let the public know the degrees to which these issues are being taken seriously within their community. Participation by public safety officials in outreach groups and Y2K preparedness meetings held by religious congregations, citizens groups, and local community groups is an effective and direct way to create a higher level of awareness in the community. Particularly successful outreach efforts have brought not only their message of preparedness and awareness but representatives from other county departments, cities departments, school districts, utilities, and volunteer groups to echo the same sentiments.

The Orange County Sheriff's Department holds regular community meetings on its Y2K status and makes newsletters available to the community in order to keep the public informed as to what progress has been made. In Kern County, the Sheriff's Department utilizes its "crime presentation unit" to make regular presentations to the community and has directed its "D.A.R.E." officers to address potential Y2K issues that may be brought up by students.

The Fresno County Fire Department is working with one of the largest movie theaters in the area, to do public service announcements in between the running of the movies with some Y2K specific material in addition to general preparedness information.

Furthermore, as mentioned in regards to city and county public awareness programs, general information is available on county and city websites, for those that have access to it. Printed information is also being included in utility bills and is available at most offices open to the public.

Finally, the California National Guard has been directed by the Department of Defense to be fully Y2K-ready by October 1st, and the Guard is already well on its way. All high frequency radios have been certified compliant by vendors. Table top exercises have been conducted and will continue, concurrently, with systems testing. Of the 1700 army guard and 4900 air guard in the state, 2 individuals will be on duty in every armory statewide and for the remaining members of the Guard, New Year's weekend has been designated as a "drill weekend."

IV. Transportation Preparedness

"Most of the hype surrounding Y2K has focused on airplanes falling out of the sky. The airlines have assured us that not only will that not happen but that no flight safety issues related to Y2K for airborne systems exist for an airplane in flight."

Tim Harris, John Wayne Airport

The Committee heard testimony from transportation agencies from most major metropolitan areas and eight of the state's ten busy international airports on their Y2K preparedness and business continuity planning efforts. The fact that most of the transportation authorities and airports have planning timelines that run their remediation programs into the last quarter of this year is somewhat disconcerting. However, since their coordinated efforts focus on end-to-end business continuity planning rather than systems integration, their planned program end dates are less problematic than other agencies'.

Transit agencies such as Muni, MTA, BART, Santa Clara Valley Transportation Authority (VTA), AC Transit, OCTA, and San Diego Metropolitan Transit, do not have major electronic data exchange partners. Where they do have external interfaces most, except utilities, have nothing to do with the direct provision of services, nor does their coordination with CalTrans or the U.S. Department of Transportation impact their day-to-day operations.

In the Bay Area, the Metropolitan Transportation Commission (MTC) has taken on the role of information clearinghouse for transit agencies and the public. In cooperation with the state Office of Emergency Services, the MTC has developed a comprehensive "TransResponse Plan" where MTC develops regional contingency plans and alternatives for the coordination of basic transportation service. The TransResopnse Plan has developed though partnership workshops on independent agency status and contingency planning for traffic control and transit systems.

The MTC also administers the freeway service patrol and highway call box programs along Bay Area highways. Remaining hurdles include remediating the radio dispatch system for tow trucks on service patrol, scheduled for August, and replacing the mother boards in 3300 call boxes that are currently Y2K non-compliant.

Among specific Bay Area providers, BART is the furthest along with remediation and testing but also has the most complex business continuity planning process since it is almost completely reliant on power from external agencies. For all other transit agencies

that provide bus and ferry services, except for Muni and VTA who also run rail systems, there are localized problems that could occur, but that will not impact the ability of buses or ferries to run. The initial concerns are with fare boxes, destination signs, GPS tracking systems, and other electronic devices on board vehicles that vendors have failed to certify as Y2K compliant. MTC has determined that complexities in certifying readiness on the rail systems maintained by Muni and VTA have rendered much of their preparedness problematic in light of the fact that, like BART, they are ultimately reliant on external agencies for power to run their light rail systems.

In Los Angeles, the MTA has made a significant amount of progress on its Y2K program itself in addition to its remediation and continuity planning efforts. Last fall before the Information Technology Committee, MTA had systems that did not have their remediation scheduled until late December of 1999. With the assistance of several vendors who have been hired on to expedite their Year 2000 work, MTA is now looking at completion of both remediation and testing by the middle of November. While November itself could prove to be too late for complete systems testing it is reassuring that the Authority has developed more aggressive approaches to Y2K.

On the other hand, the transit agencies serving Orange County and San Diego both seem to have done a considerable amount of heavy lifting on the Year 2000 Problem. OCTA, for example, began its infrastructure assessment and inventory program in 1996, and by April of this year all mission critical networking and communications infrastructure was remediated, tested and put back into production. OCTA is currently running tests with 11 outside entities that it exchanges data with on a non-mission critical basis: banks, credit unions, and retirement systems.

Turning now to airports, with the assurance that planes will not be dropping out of the sky major issues still remain. During the course of our hearings we were given testimony regarding preparedness activities and business continuity planning by Burbank-Glendale-Pasadena (BUR), Fresno Yosemite (FYI), Los Angeles (LAX), Oakland (OAK), Orange County (John Wayne), San Diego (SAN), San Francisco (SFO), and San Jose (SJC) International Airports.

Although not a commercial airport, the following potential scenario at the municipal Santa Monica Airport was presented to the Committee by the City of Santa Monica. It makes a very strong case for ironclad business continuity planning at our airfields:

> "The FAA control tower has a backup power source if there is a citywide electrical power outage. That generator has sufficient fuel to provide electrical power to the control tower for three days. After which, a power outage would affect the airport in the following manner: there would be no runway lights; no taxi way lights; no runway end identifier lights; no precession approach path indicator to coordinate NFR and IFR approaches; no visual approach slope indicator lights; no airport rotator beacon."

FAA-mandated business continuity plans are already in place at all airports, but the plans are not required to be Y2K-specific.

Airports must manage a complicated set of interdependent responsibilities in coordination with the FAA, and airlines. Generally, during remediation they own the following:

The Airport:	Runway lights, emergency power, access control, building controls, paging, and crash, fire and rescue.
The Airlines:	Planes, fueling, security screening, jetways, baggage handling, and ticketing.
The FAA:	Air traffic control, navigational aids, and the tower.

At John Wayne, these responsibilities translate into the following ownership workload as a percentage of effected systems: 3.8% FAA, 16% Airlines, 79.2% Airport and Local Government.

Santa Monica Airport was not the only airfield with potential airfield lighting problems. SFO replaced their previous airfield lighting system when it was found to be non-compliant. Initial assessments and inventorying at FYI determined that their airfield lighting control system was not Y2K compliant and the airport is currently in the process of installing a new one. LAX did not have a compliance with their lighting issues, nor were any reported at OAK or SAN. BUR still has a manual lighting system in place and at John Wayne the FAA controls airfield lighting from the tower. A rumor had made it to the State Capitol last winter regarding the failure of the airfield lighting during integrated systems testing at SJC, however when confronted by the Committee that rumor was vehemently denied.

Remediation and testing schedules show that several airports have scheduled project completion into the fourth quarter of this year. Most notably, SAN and OAK seem to be behind the compliance curves set by their peers. SAN has not scheduled completion of its remediation program until October and does not expect to finish testing until November. OAK meanwhile has spent $2.2 million on their program which began in earnest in January of 1998, but as of March was still only 20% complete.

At this time, no California airports will have the direct benefit of an end-to-end test like the one conducted at the Denver International Airport by the FAA and major airlines. The FAA will only be conducting these exercises at a select few airports and then direct the remaining airports to compare their compliance efforts to those found to be successful based on the tests and subsequent observations.

V. Utility Preparedness

"The utilities' implementation plans are on schedule or, in many cases, ahead of schedule."

Brian Schumacher, Public Utilities Commission

"When we take a look at the information we have internally through assessment, remediation, and validation, or externally through communication with our business partners, we do not have any information that leads us to believe that there are going to be any outages."

Jim Silva, Pacific Gas & Electric Co.

The utility industry faces the same Y2K challenges as every other industry. Y2K anomalies could lead to the malfunction of software programs on mainframe computers, servers, PC's, and communications system. Corrupted data may be sent from one application to another, causing incorrect results or shutdowns.

In most industries, these risks of failure mean that those automated systems used for accounting, administration, billing, and other important functions could experience problems. In the utility industry, these risks of failure mean that millions of Californians, businesses, and government officials could lose power, telecommunications, or water.

The California Public Utilities Commission (PUC) has played an active role in ensuring that the electrical utilities and telecommunications providers under their purview are taking appropriate Y2K remediation, risk reduction, and contingency planning actions. The PUC required utilities to submit an initial filing of compliance earlier this year, which are regularly updates, and then copies of their business continuity plans on July 1st. By November 1st, the PUC is requiring that each utility must certify in writing whether they are Y2K compliant or not.

Because the PUC has general regulatory authority over the utility industry, should the utilities turn out not to be as well prepared as their plans have indicated then the PUC can investigate and impose sanctions. PUC general sanctioning authority ranges from $500 to $20,000 per violation. According to PUC counsel, if a failure occurs that affects 100,000 customers, sanctions for each of the 100,000 cases may be in order, should a report have been in error.

In addition, the utilities are working with North American Electric Reliability Council (NERC), Federal Communications Commission (FCC), Western Systems Coordinating

Council (WSCC), and the National Association of Regulatory Utility Commissioners (NARUC). Utilities have been sharing information with these organizations in order to help create an environment where providers feel comfortable coordinating efforts in order to minimize the likelihood of potential disruptions.

Recognizing the importance of joint business continuity planning and tabletop exercises, NERC has assumed the primary role in monitoring the overall Y2K preparedness of the electric power industry. On April 9, 1999, NERC facilitated a drill for utility providers across North America simulating the partial loss of voice and data communications at over two hundred electric power organizations. The results from this drill were to be reflected in business continuity plans still under development by utilities, which are to be thoroughly exercised in another drill planned for September 9th.

Closer still to home, the newly formed California Independent System Operator (ISO) has been closely monitoring Y2K progress among utilities and is itself Y2K ready. The ISO's automated systems are all relatively new and have been certified as Y2K compliant. The ISO has also been hard at work developing continuity plans designed to limit the likelihood that a localized outage creates "cascading outages" throughout the system. These plans include having all operations and support personnel on-site.

All electric utility providers, both municipal and privately held, have a completion window of June to September. However, specific issues remain outstanding for providers. Pacific Gas & Electric scheduled completion of its systems remediation and testing in June, but will not certify its Year 2000 readiness until September, citing a lack of response from critical suppliers about their own readiness. City of Los Angeles, Department of Water and Power, likewise, had all network remediation and upgrades on schedule for June 30th, but had not completed all of the data formatting and bridging necessary to trade data with each of 160 external interface partners.

Likewise, the PUC has taken an active interest in monitoring the progress of California's telecommunications providers' Y2K preparedness. Reports filed with the PUC showed that effective Y2K compliance was expected by each telecommunications in the period of the end of the second quarter through September.

Four telecommunications companies serve 99.7% of California's phone customers, and, according to the FCC, these companies have completed most of their Y2K fixes and business continuity plans that will enable them to respond quickly to isolated disruptions.

The scope of the projects being undertaken by these providers is quite expansive. Expecting to spend over $125 million in California alone on Y2K readiness, Pacific Bell has completed over 95% of its work on 140 million lines of code, 13,000 programs and products, 2800 facilities, and interfaces with some 1200 vendors. GTE had spent somewhere around $370 million across the corporation to reach a 99% completion rate; in the State of California, 4.6 million access lines have been certified compliant, representing all of their service exchanges, except for some residual work that remained to be completed in Weaverville.

As mentioned earlier, 911 system readiness is primarily the responsibility of phone companies and the local governments that actively use the equipment. The first step of assessment of 911 readiness has been the compliance or non-compliance of equipment delivered by the manufacturer. Once this has been determined, then the phone company must physically visit each "answering point" across the state to work with the local officials to complete a thorough inventory at that site. In several instances, 911 systems have had to be completely replaced after inventorying; the new 911 dispatch system in Fresno (Pacific Bell Palladium System by Lucent Technologies) is one of the most advanced systems in the entire country and is unique in the State of California.

For many local governments and companies that operate major water and waste water utilities, Y2K may be a major operational issue depending on whether or not there are a significant number of embedded chips in the delivery process.

Many water departments have automated systems, controlled by microprocessors, called SCADA (Supervisory Control and Data Acquisition). SCADA systems monitor, control and process variables at remote locations and then record that data for historical purposes. These systems actively monitor reservoir levels, water quality, water pressure, pump station activities, and decide if and when a pump needs to be turned on or off, based on the flow capacity of the aqueduct or channel.

Regardless of the fact that most SCADA vendors have certified system compliance, municipalities and water companies have essentially the same business continuity plans in place as those providers without embedded systems problems. All water system business continuity plans have the same basic principal guiding their development: that gravity is Y2K compliant. Staff will be standing by to operate systems as they were prior to automation to watch gauges and turn knobs.

Sewer stations have similar continuity planning requirements as water pumping stations. The highest level of automation surrounds air compressors, which if they have been automated, can have operations that are microprocessor based. While these microprocessors could have an embedded systems problem like any other, air compressors have manual by-pass valves and once again, staff is going to be ready to deal with those situations.

Electric and telecommunications companies have been key partners in federal, state, and local government Y2K business continuity planning efforts. Generic provisions of these plans include having additional employees on duty at key operational and administrative locations. Additional stand-by staff will be on call and ready to respond on 30-minutes notice in most locations, as well.

Like public safety agencies, they base the success of previous contingency planning efforts on their performance and the issues that were identified during previous disasters. The Los Angeles Department of Water & Power has incorporated lessons from their experiences with the Northridge earthquake to help them prepare from any problems that may arise on January 1st. SMUD has built into its business continuity plans not only the

lessons it has learned from dealing with major floods but also the district's basic readiness for floods during winter months.

Municipal utilities, such as City of Santa Clara, Silicon Valley Power, have also been an integral part of initiating community planning exercises. Silicon Valley Power had planned three tabletop drills that reflect the regional focus of a municipal provider. The first exercise in June was scheduled to include school districts, hospitals, city agencies and Santa Clara County. The City of Anaheim's Public Utilities Department, has adopted the philosophy that as a utility it operates in an emergency response environment all the time. It is advising other city departments and residents that city utilities are simply overhauling existing plans to immediately address and respond to electric and water failures that may be associated with Y2K.

Unfortunately, the utility industry has failed to do a very good job in its public awareness efforts. In order to make the general public, local governments, and the media, at large, aware of how much time, energy, and resources they have devoted to their extremely successful remediation plans utilities need to devote yet more time and resources to Y2K.

To this point in time, utilities have primarily relied on Y2K bill inserts to serve as their primary method of public awareness. Every utility that testified before the Committee has produced a brochure or other form of insert to accompany billings sent to customers. Yet, customers do not always pay attention to inserts, nor do inserts get read by all residents or employees at the address to which bills are sent.

In order to remedy these deficiencies, utilities need to establish an aggressive public awareness campaign as soon as possible. Electric and telecommunications providers who have existing public relations strategies should accelerate their timelines. Final systems testing and the resolution of issues should be presented to the media as often as possible. Utilities should act to be more pro-active with local governments and citizens groups by offering staff to lead community discussions regarding Y2K preparedness, contributing time and resources to local government community preparedness public awareness and outreach campaigns, and developing direct relationships with local reporters who may be covering potential Y2K failures on New Year's Eve, 1999.

Appendices

Appendix A:	Committee Hearing Agendas
Appendix B:	City Presentations & Reports
Appendix C:	County Presentations & Reports
Appendix D:	Public Safety Presentations & Reports
Appendix E:	Transportation Presentations & Reports
Appendix F:	Utility Presentations & Reports
Appendix G:	Public Awareness Brochures and Pamphlets
Appendix H:	Budgeted Year 2000 Funding Levels
Appendix I:	Association of Bay Area Governments (ABAG) Presentation on Local Government Liability
Appendix J:	Department of Information Technology (DOIT) County Interfaces by State Department
Appendix K:	Committee Preparedness Metrics
Appendix L:	Year 2000 Problem Overview, February 1999
Appendix M:	Executive Order D-3-99